

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
6 février 2003 (06.02.2003)

PCT

(10) Numéro de publication internationale
WO 03/010720 A2

(51) Classification internationale des brevets⁷ : **G07F** (81) États désignés (*national*) : AB, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(21) Numéro de la demande internationale : **PCT/FR02/02657**

(22) Date de dépôt international : 24 juillet 2002 (24.07.2002)

(25) Langue de dépôt : **français**

(26) Langue de publication : **français**

(30) Données relatives à la priorité :
01 09904 25 juillet 2001 (25.07.2001) FR.
01 09903 25 juillet 2001 (25.07.2001) FR

(84) États désignés (*régional*) : brevet ARPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), brevet OAPI (BF, BJ, CR, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(71) Déposant (*pour tous les États désignés sauf US*) :
CREDIT LYONNAIS (FR/FR); 18 rue de la République,
F-69002 LYON (FR).

Publiée :
— sans rapport de recherche internationale, sera republiée
dès réception de ce rapport

(72) Inventeurs ; et

(75) Inventeur/Déposant (*pour US seulement*) : **BERGSTEN, Ulrik** (FR/FR); 17 rue Louis Maurice, F-94210 LA VARENNE (FR). **ASSERUS, Frédéric** (FR/FR); River Side, 74 rue Camille Claudel, F-78955 CARRIERES SOUS POISSY (FR).

(74) Mandataire : **GRYNWALD, Albert**; Cabinet GRYNWALD, 127 rue du Faubourg Poissonnière, F-75009 PARIS (FR).

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) Titre: METHOD AND SYSTEM USING A USER PORTABLE DEVICE FOR VALIDATING A REQUEST WITH AN ENTITY

(54) Titre : PROCÉDÉ ET SYSTÈME PERMETTANT DE VALIDER, EN METTANT EN ŒUVRE UN OBJET PORTABLE D'UN UTILISATEUR, UNE REQUÊTE AUPRÈS D'UNE ENTITÉ

(57) **Abstract:** The invention concerns a method and a system enabling a user (2) to perform remote payment settlement for goods and/or services. The method comprises: a step whereby the user (2) transmits to an acceptor trader (23) supplying goods and/or services, a personal identifier, in particular consisting of a call number (22) of the mobile telephone (25) of the user (2); a step whereby the user (2) transmits a password (15) to a banking institution (7). When the user (2) is registered, the password (15) is transmitted, by the banking institution (7) to the user (2) entirely or partly via a terminal (8), in particular an ATM/ABM automatic cash dispensing machine. The payment for the goods and/or services is thus settled remotely by the user (2).

(57) **Abstrait :** L'invention concerne un procédé et un système permettant à un utilisateur (2) d'acquitter à distance le paiement de biens et/ou services. Le procédé comprend : - l'étape, pour l'utilisateur (2), de transmettre, à un commerçant accepteur (23) fournissant les biens et/ou services, un identifiant personnel, notamment constitué du numéro d'appel (22) du téléphone mobile (25) de l'utilisateur (2), - l'étape, pour l'utilisateur (2), de transmettre, directement ou indirectement, un mot de passe (15) à un organisme bancaire (7). Lors d'une phase d'enregistrement de l'utilisateur (2), le mot de passe (15) a été transmis, par l'organisme bancaire (7) à l'utilisateur (2), en tout ou partie via un terminal (8), notamment un distributeur automatique de billets de banque du type DAB/GAB. Le paiement des biens et/ou services est ainsi acquitté à distance par l'utilisateur (2).

WO 03/010720 A2

PROCEDE ET SYSTEME PERMETTANT DE VALIDER, EN METTANT EN OUVRE UN
OBJET PORTABLE D'UN UTILISATEUR, UNE REQUETE AUPRES D'UNE ENTITE

Préambule de la description

Domaine concerné, problème posé

La présente invention concerne un procédé et un système permettant de valider, en mettant en œuvre un objet portable d'un utilisateur, qu'une requête auprès d'une entité émane de l'utilisateur. La présente invention concerne également un procédé et un système destiné à permettre à un utilisateur d'effectuer un paiement à distance auprès d'un accepteur.

Le développement du commerce électronique grand public, c'est à dire la commercialisation de produits ou de services à partir d'un site commercial représenté typiquement par un serveur sur Internet reste freiné par l'absence de moyens ou de modes de paiement adaptés à de telles situations.

Les moyens de paiement disponibles de façon à peu près universelle souffrent de différents types de problèmes.

(a) Le chèque ne se prête pas à la dématérialisation et suppose l'envoi, ultérieur à la passation d'une commande, d'un courrier contenant le chèque.

(b) La carte bancaire n'est encore utilisable à grande échelle que dans le cadre d'un mode de vente à distance qui impose à l'utilisateur de communiquer au commerçant, à titre de

paiement, le numéro de sa carte bancaire et des informations liées à sa carte bancaire, notamment la date d'expiration et éventuellement un cryptogramme visuel.

(c) Les banques et notamment les banques françaises 5 ont cherché à développer un mode de paiement basé sur la carte bancaire et censé être adapté au commerce électronique grand public : c'est le télépaiement sécurisé sous différentes formes techniques. Le télépaiement sécurisé propose une solution qui se rapproche du paiement de proximité par carte bancaire. Il offre 10 aux commerçants une garantie de paiement. En effet, ce mode de paiement est construit pour interdire la réputation des paiements par les utilisateurs.

En mode de vente à distance, le commerçant bénéficie 15 auprès de sa banque d'une garantie de paiement contre certains risques, notamment l'inexistence de la carte, la carte en opposition, déclarée perdue ou volée, l'utilisateur insolvable au moment du paiement. Il subsiste néanmoins le risque de réputation dans le cas où le titulaire de la carte utilisée pour le paiement conteste le paiement, c'est à dire qu'il 20 déclare formellement qu'il n'a pas effectué le paiement considéré. La solution utilisée couramment pour se prémunir contre la première catégorie de risques est la technique de la demande d'autorisation. L'objet du télépaiement sécurisé est de compléter la garantie accordée par la demande d'autorisation en 25 éliminant le risque de réputation. On utilise pour cela la puce présente dans les cartes bancaires. La puce va générer une « signature électronique » qui sera associée au paiement et qui montrera que la responsabilité du titulaire de la carte est bien engagée.

30 Le problème resté jusqu'à présent insurmontable vient du fait que la valeur d'usage du télépaiement sécurisé reste faible tant que l'on n'a pas réussi à généraliser simultanément le support du télépaiement tant du côté des utilisateurs que des commerçants. En effet, tant que l'on reste loin d'une telle 35 généralisation, la motivation des utilisateurs comme celle des

commerçants reste très limitée. Les contraintes liées à sa mise en œuvre ne sont pas négligeables, notamment le coût et la difficulté d'utilisation. Pour un commerçant, l'acceptation du mode télépaiement sécurisé ne suffit pas car pour développer son activité, il doit être en mesure d'accepter des paiements de la grande majorité des internautes. De ce fait, il doit continuer à accepter des paiements en mode de vente à distance. Mais malheureusement, dans ces conditions il ne verra pratiquement pas le taux de ses impayés baisser car ces impayés, seront motivés par la répudiation d'une partie des paiements. La totalité des fraudeurs choisiront en effet logiquement le mode de paiement le moins sécurisé. Du côté de l'utilisateur, accéder au télépaiement sécurisé nécessite un effort non négligeable, notamment l'acquisition coûteuse d'un lecteur de carte bancaire, une installation sur un poste de travail, un temps d'apprentissage, alors que ce mode de paiement ne lui apporte rien de tangible directement. Autrement dit, tant que la quasi-totalité des commerçants accepteront d'être payés en mode vente à distance l'utilisateur ne percevra pas l'intérêt d'un tel effort.

La présente invention ne prétend pas être un mode de paiement similaire ou équivalent aux différentes formes de télépaiement sécurisé. La présente invention cherche à apporter aux commerçants une solution meilleure que la vente à distance traditionnelle et qui soit plus rapidement applicable que le mode de télépaiement sécurisé.

On peut classer en trois catégories les motifs pour lesquels une transaction est répudiée :

- le paiement est effectué par un tiers qui a réussi à se procurer un numéro de carte (et la date d'expiration, voire même le cryptogramme visuel),
- le commerçant n'a pas donné entière satisfaction au client,
- le client est réellement de mauvaise foi en répudiant le paiement.

Le procédé et le système selon l'invention cherche à éliminer le premier motif de répudiation ou au moins à en réduire très fortement la probabilité. Par contre, déresponsabiliser les commerçants en les protégeant contre le deuxième motif d'impayé ne conduit qu'à une accentuation des problèmes. Enfin, et contrairement au télépaiement sécurisé, le procédé et le système selon l'invention n'apportent pas de garantie formelle contre le troisième motif de répudiation mais les clients hésiteront néanmoins à tricher car ils auront le sentiment qu'on risque de pouvoir les confondre.

La présente invention a pour objet de réduire de façon significative sinon d'éliminer le risque principal de répudiation d'une transaction, à savoir la répudiation du fait de la fraude d'un tiers qui a réussi à se procurer un numéro de carte et la date d'expiration correspondante, voire le cryptogramme visuel.

La présente invention a pour objet de permettre aux commerçants qui la mettent en œuvre de réduire leur taux d'impayés et de ne plus avoir à utiliser le mode vente à distance classique en subissant les inconvénients ci-dessus explicités.

La présente invention a pour objet de procurer aux utilisateurs qui la mettent en œuvre un niveau de confiance très élevé. En effet, les utilisateurs ont la double assurance que leur numéro de carte bancaire ne risque pas d'être détourné et qu'aucun fraudeur ne peut payer, en utilisant un numéro de carte qui n'est pas le sien, chez les commerçants mettant en œuvre la présente invention.

Le procédé selon l'invention

L'invention concerne d'une manière générale un procédé permettant de valider qu'une requête auprès d'une entité émane d'un utilisateur. L'invention concerne plus particulièrement, ainsi que cela sera ci-après exposé, un procédé destiné à permettre à un utilisateur, d'effectuer un paiement à distance auprès d'un accepteur.

Dans sa forme générale, l'invention met en œuvre un objet portable mis à la disposition d'un utilisateur. L'objet portable se présente notamment sous la forme d'une carte bancaire. La requête porte notamment sur une transaction ou des informations confidentielles relatives à l'accès à un service ou à un lieu. On peut distinguer trois phases :

- une phase d'enregistrement au cours de laquelle l'utilisateur s'enregistre auprès d'un organisme, notamment un organisme bancaire,

10 - une phase d'émission d'une requête,

- une phase d'autorisation de réponse à la requête.

Phase d'enregistrement

Lors de la phase d'enregistrement d'un utilisateur auprès d'un organisme, notamment un organisme bancaire le procédé met en œuvre les étapes suivantes :

15 L'étape, pour l'utilisateur, d'accoupler l'objet portable à un terminal, notamment de type distributeur automatique de billets (DAB-GAB) ou de type terminal de paiement électronique (TPE). Le terminal est connecté de manière directe ou indirecte à un serveur associé à une base de données de l'organisme.

20 Lors de la phase d'enregistrement, sur requête du terminal, l'utilisateur entre dans le terminal des données d'authentification de l'utilisateur, notamment un code confidentiel et/ou des données bio-métriques, associées à l'objet portable. Le terminal vérifie que les données d'authentification de l'utilisateur correspondent à l'objet portable.

25 Il résulte de la combinaison des traits techniques que la phase d'enregistrement permet d'authentifier l'objet portable et de vérifier que l'utilisateur est bien le titulaire de l'objet portable.

30 Lors de la phase d'enregistrement sur requête du terminal, l'utilisateur compose, au moyen d'un clavier du terminal, un identifiant personnel, notamment le numéro d'appel

de son téléphone mobile. l'identifiant personnel est transmis par le terminal au serveur. Le terminal transmet un mot de passe à l'utilisateur, notamment en affichant le mot de passe sur un écran du terminal ou en délivrant à l'utilisateur un ticket sur lequel est imprimé le mot de passe. le mot de passe a été déterminé par le serveur et transmis au terminal. Il résulte de la combinaison des traits techniques que le mot de passe attribué par le serveur ne peut être transmis qu'à l'utilisateur titulaire de l'objet portable authentifié.

10 Lors de la phase d'enregistrement, le serveur mémorise et associe dans la base de données de l'organisme :

- l'identifiant personnel,
- le mot de passe.

Phase d'émission d'une requête

15 Lors d'une phase d'émission d'une requête concernant notamment des informations confidentielles, l'utilisateur transmet à l'entité :

- la requête,
- l'identifiant personnel, notamment le numéro d'appel associé au téléphone mobile.

Phase d'autorisation de réponse à la requête

Le procédé selon l'invention comprend en outre, lors d'une phase d'autorisation de réponse à la requête, les étapes qui seront ci-après décrites :

25 L'entité transmet à l'organisme l'identifiant personnel.

L'organisme adresse à l'utilisateur un message, notamment de type SMS. le message comprend une requête de saisie du mot de passe, se présentant notamment sous la forme d'un champ de saisie dans le message.

30 L'utilisateur transmet en retour le mot de passe à l'organisme, notamment en saisissant le mot de passe dans le champ de saisie.

35 L'organisme vérifie, dans la base de données, que le mot de passe, transmis par l'utilisateur, correspond à un mot de

passe associé à l'identifiant personnel transmis par l'entité. Puis, l'organisme autorise l'entité à répondre à la requête de l'utilisateur.

De préférence, selon l'invention, le procédé est tel qu'il comprend en outre, lors de la phase d'enregistrement, l'étape, pour le terminal, de lire dans l'objet portable et de transmettre au serveur des données, notamment le numéro et la date d'expiration de l'objet portable ainsi que le nom et le prénom du titulaire de l'objet portable.

10 Il résulte de la combinaison des traits techniques décrits que la réponse à la requête est transmise par l'entité à l'utilisateur sans que l'entité ait eu connaissance du numéro et de la date d'expiration de l'objet portable de l'utilisateur.

De préférence, selon l'invention, le procédé est tel qu'il comprend en outre l'étape, pour le serveur, (i) de mémoriser et d'associer dans la base de données de l'organisme les données, notamment le numéro et la date d'expiration de l'objet portable, et (ii) d'associer les données avec l'identifiant personnel et le mot de passe.

20 De préférence, selon l'invention, le procédé est tel que l'identifiant personnel est une adresse de l'utilisateur à laquelle l'organisme peut transmettre la requête de saisie du mot de passe. L'adresse peut être notamment un numéro de téléphone mobile ou fixe ou une adresse de messagerie électronique. Il résulte de la combinaison des traits techniques que, selon toute vraisemblance, le message ne peut être reçu que par l'utilisateur.

De préférence, selon l'invention, le procédé comprend en outre l'étape, pour l'organisme, de vérifier que l'utilisateur peut être contacté à l'adresse définie par l'identifiant personnel, lors d'une requête relative à l'identifiant personnel.

Cas du paiement de biens ou de services

30 L'invention concerne plus particulièrement un procédé destiné à permettre à un utilisateur, disposant d'un objet

portable et d'un terminal mobile ayant une fonction de téléphonie, d'effectuer un paiement à distance auprès d'un accepteur. L'objet portable se présente notamment sous la forme d'une carte bancaire.

5 On peut distinguer deux phases :

- une phase d'enregistrement au cours de laquelle l'utilisateur s'enregistre auprès d'un organisme, notamment un organisme bancaire,
- une phase de paiement.

10 **Phase d'enregistrement**

Lors de la phase d'enregistrement d'un utilisateur auprès d'un organisme, notamment un organisme bancaire le procédé met en œuvre les étapes suivantes :

15 L'utilisateur d'accouple l'objet portable à un terminal, notamment de type distributeur automatique de billets (DAB-GAB) ou de type terminal de paiement électronique (TPE). Le terminal est connecté de manière directe ou indirecte à un serveur associé à une base de données de l'organisme.

20 Sur requête du terminal, l'utilisateur entre dans le terminal des données d'authentification de l'utilisateur, notamment un code confidentiel et/ou des données bio-métriques, associées à l'objet portable.

Le terminal vérifie que les données d'authentification de l'utilisateur correspondent à l'objet portable.

25 Il résulte de la combinaison des traits techniques ci-dessus décrits que la phase d'enregistrement permet d'authentifier l'objet portable et de vérifier que l'utilisateur est bien le titulaire de l'objet portable.

30 Le procédé comprend en outre, lors de la phase d'enregistrement, les étapes suivantes :

Le terminal lit dans l'objet portable et transmet au serveur des données d'identification, notamment le numéro et la date d'expiration de l'objet portable ainsi que le nom et le prénom du titulaire de l'objet portable.

Sur requête du terminal, l'utilisateur compose, au moyen d'un clavier du terminal, le numéro d'appel associé au terminal mobile.

le numéro d'appel associé au terminal mobile est
5 transmis, par le terminal, au serveur.

le terminal transmet un mot de passe à l'utilisateur, notamment en affichant le mot de passe sur un écran du terminal ou en délivrant à l'utilisateur un ticket sur lequel est imprimé le mot de passe. le mot de passe a été déterminé par le serveur et transmis au terminal.
10

Il résulte de la combinaison des traits techniques que le mot de passe attribué par le serveur ne peut être transmis qu'à l'utilisateur titulaire de l'objet portable authentifié.

Lors de la phase d'enregistrement le serveur mémorise
15 et associe, dans la base de données de l'organisme :

- les données d'identification,
- le numéro d'appel associé au terminal mobile,
- le mot de passe.

Phase de paiement

20 Lors de la phase de paiement, le procédé selon l'invention met en œuvre les étapes suivantes :

L'utilisateur transmet à l'accepteur le numéro d'appel associé au terminal mobile.

L'accepteur transmet à l'organisme le numéro d'appel
25 associé au terminal mobile ainsi que des informations relatives au paiement, dont le montant du paiement..

L'organisme adresse à l'utilisateur un message, notamment de type SMS, en utilisant le numéro d'appel associé au terminal mobile.

30 le message comprend :

- les informations relatives au paiement,
- une requête de saisie du mot de passe, se présentant notamment sous la forme d'un champ de saisie dans le message.

.10

L'utilisateur transmet en retour le mot de passe à l'organisme, notamment en saisissant le mot de passe dans le champ de saisie.

5 L'organisme vérifie, dans la base de données, que le mot de passe transmis par l'utilisateur correspond au numéro d'appel associé au terminal mobile transmis par l'accepteur.

L'organisme :

- (i) recherche, dans la base de données, tout ou partie des données d'identification, notamment le numéro et la date d'expiration de l'objet portable, correspondant au numéro d'appel associé au terminal mobile et au mot de passe,
- (ii) fait débiter ou débite un compte bancaire associé à l'objet portable du montant du paiement et fait créditer ou crédite l'accepteur du montant,
- 15 • (iii) confirme auprès de l'accepteur le paiement à distance de l'utilisateur.

De préférence, l'organisme vérifie la validité de l'objet portable avant de confirmer à l'accepteur le paiement à distance de l'utilisateur.

20 Il résulte de la combinaison des traits techniques que le paiement est acquitté à distance par l'utilisateur sans qu'il ait eu à communiquer à l'accepteur les données d'identification de l'objet portable, notamment le numéro et de la date d'expiration de la carte bancaire de l'utilisateur.

25 **Le système selon l'invention**

L'invention concerne également d'une manière générale un système permettant de valider qu'une requête auprès d'une entité émane d'un utilisateur. L'invention concerne plus particulièrement, ainsi que cela sera ci-après exposé, un système destiné à permettre à un utilisateur, d'effectuer un paiement à distance auprès d'un accepteur.

Dans sa forme générale, l'invention met en œuvre un objet portable mis à la disposition d'un utilisateur. l'objet portable se présente notamment sous la forme d'une carte bancaire. la requête porte notamment sur une transaction ou sur

des informations confidentielles relatives à l'accès à un service ou à un lieu.

On peut distinguer trois phases impliquant la mise en œuvre de moyens techniques spécifiques :

5 - une phase d'enregistrement au cours de laquelle l'utilisateur s'enregistre auprès d'un organisme, notamment un organisme bancaire,
- une phase d'émission d'une requête,
- une phase d'autorisation de réponse à la requête.

10 Phase d'enregistrement de l'utilisateur auprès d'un organisme, notamment un organisme bancaire

Le système comprend, pour permettre l'enregistrement de l'utilisateur, un terminal, notamment un terminal de type distributeur automatique de billets (DAB-GAB) ou de type 15 terminal de paiement électronique (TPE). Le terminal comporte des moyens d'accouplement permettant à l'utilisateur d'accoupler l'objet portable au terminal.

Le système comprend en outre un serveur associé à une base de données d'un organisme, notamment un organisme bancaire.

20 le serveur comprend des moyens de connexion pour connecter, de manière directe ou indirecte, le terminal au serveur via un réseau de communication, notamment informatique. le terminal comprend une interface utilisateur-terminal permettant à l'utilisateur d'entrer dans le terminal, sur 25 requête du terminal, des données d'authentification de l'utilisateur, notamment un code confidentiel et/ou des données bio-métriques, associées à l'objet portable. Le terminal comprend en outre des moyens de vérification terminal pour vérifier que les données d'authentification de l'utilisateur 30 correspondent à l'objet portable.

Il résulte de la combinaison des moyens techniques décrits que la phase d'enregistrement permet d'authentifier l'objet portable et de vérifier que l'utilisateur est bien le titulaire de l'objet portable.

L'interface utilisateur-terminal comporte un clavier permettant à l'utilisateur de composer, sur requête du terminal, un identifiant personnel, notamment le numéro d'appel d'un téléphone mobile de l'utilisateur.

5 le terminal comporte en outre :
 - des moyens de transmission terminal pour transmettre
 l'identifiant personnel au serveur,
 - des moyens de communication terminal pour
 communiquer un mot de passe à l'utilisateur, notamment en
10 affichant le mot de passe sur un écran du terminal ou en
 délivrant à l'utilisateur un ticket sur lequel est imprimé le
 mot de passe.

le mot de passe a été déterminé par le serveur en
mettant en œuvre des moyens de traitement informatique serveur.
15 le mot de passe a été transmis par le serveur au terminal, via
 le réseau de communication.

Il résulte de la combinaison des moyens techniques
décris que le mot de passe attribué par le serveur ne peut être
transmis qu'à l'utilisateur titulaire de l'objet portable
20 authentifié. les moyens de traitement informatique serveur
comportent des moyens d'enregistrement pour mémoriser et
associer dans la base de données :

25 - l'identifiant personnel,
 - le mot de passe.

Phase d'émission d'une requête par un utilisateur
Le système comprend en outre des moyens
d'établissement de requête et de transmission de requête
permettant à l'utilisateur d'émettre une requête, concernant
notamment des informations confidentielles, et de transmettre à
30 l'entité la requête ainsi que l'identifiant personnel, notamment
 le numéro d'appel associé au téléphone mobile.

Phase d'autorisation de réponse à la requête
Les moyens techniques ci-après décrits sont mis en
œuvre lors de la phase d'autorisation de réponse à la requête.
35 Le serveur de l'organisme comprend en outre :

- des moyens de réception serveur pour recevoir de l'entité l'identifiant personnel,
- des moyens de transmission serveur pour adresser à l'utilisateur un message, notamment de type SMS.

5 le message comprend une requête de saisie du mot de passe se présentant notamment sous la forme d'un champ de saisie dans le message.

10 L'utilisateur dispose de moyens de transmission de mot de passe, notamment d'un téléphone mobile, permettant, à l'utilisateur, de transmettre en retour le mot de passe au serveur de l'organisme, après que le mot de passe ait été saisi par l'utilisateur dans le champ de saisie.

15 les moyens de traitement informatique serveur comporte des moyens de vérification serveur pour vérifier dans la base de données que le mot de passe, transmis par l'utilisateur, correspond à un mot de passe associé à l'identifiant personnel transmis par l'entité. le serveur produit, en cas de vérification aboutie, un message d'autorisation destiné à être transmis à l'entité, l'autorisant à répondre à la requête de 20 l'utilisateur.

De préférence, selon l'invention le système est tel que le terminal comprend :

25 - des moyens de lecture terminal permettant de lire dans l'objet portable des données, notamment le numéro et la date d'expiration de l'objet portable ainsi que le nom et le prénom du titulaire de l'objet portable,

- des moyens de transmission terminal permettant de transmettre les données au serveur.

30 les moyens de lecture terminal et les moyens de transmission terminal sont mis en œuvre lors de la phase d'enregistrement de l'utilisateur.

De préférence, selon l'invention, le système est tel que les moyens d'enregistrement du serveur permettent de mémoriser dans la base de données et d'associer avec

l'identifiant personnel et le mot de passe, les données, notamment le numéro et la date d'expiration de l'objet portable.

De préférence, selon l'invention, le système est tel que l'identifiant personnel est une adresse de l'utilisateur à laquelle l'organisme peut transmettre la requête de saisie du mot de passe. L'adresse peut être notamment un numéro de téléphone mobile ou fixe ou une adresse de messagerie électronique. Il résulte de la combinaison des moyens techniques décrits que, selon toute vraisemblance, le message ne peut être reçu que par l'utilisateur.

De préférence, selon l'invention, le système est tel que les moyens de traitement informatique et les moyens de transmission serveur permettent de vérifier que l'utilisateur peut être contacté à l'adresse définie par l'identifiant personnel.

Cas du paiement de biens ou de services

L'invention concerne plus particulièrement un système permettant à un utilisateur, disposant d'un objet portable et d'un terminal mobile ayant une fonction de téléphonie, d'effectuer un paiement à distance auprès d'un accepteur. L'objet portable se présente notamment sous la forme d'une carte bancaire.

On peut distinguer deux phases impliquant la mise en œuvre de moyens techniques spécifiques :

- une phase d'enregistrement au cours de laquelle l'utilisateur s'enregistre auprès d'un organisme, notamment un organisme bancaire,

- une phase de paiement.

Phase d'enregistrement de l'utilisateur auprès d'un organisme, notamment auprès d'un organisme bancaire

Le système comprend, pour permettre l'enregistrement de l'utilisateur, un terminal, notamment un terminal de type distributeur automatique de billets (DAB-GAB) ou de type terminal de paiement électronique (TPE). Le terminal comporte

des moyens d'accouplement permettant à l'utilisateur, d'accoupler l'objet portable au terminal.

Le système comprend en outre un serveur associé à une base de données d'un organisme, notamment d'un organisme bancaire.

le serveur comprend des moyens de connexion pour connecter, de manière directe ou indirecte, le terminal au serveur via un réseau de communication, notamment informatique.

le terminal comprend en outre :

- 10 - une interface utilisateur-terminal permettant à l'utilisateur d'entrer dans le terminal, sur requête du terminal, des données d'authentification de l'utilisateur, notamment un code confidentiel et/ou des données bio-métriques, associées à l'objet portable,

- 15 - des moyens de vérification terminal pour vérifier que les données d'authentification de l'utilisateur correspondent à l'objet portable.

Il résulte de la combinaison des traits techniques que la phase d'enregistrement permet d'authentifier l'objet portable
20 et de vérifier que l'utilisateur est bien le titulaire de l'objet portable.

le terminal comprend en outre :

- des moyens de lecture terminal permettant de lire dans l'objet portable des données d'identification, notamment le numéro et la date d'expiration de l'objet portable ainsi que le nom et le prénom du titulaire de l'objet portable,

- des moyens de transmission terminal permettant de transmettre les données au serveur.

Les moyens de lecture terminal et les moyens de transmission terminal sont mis en œuvre lors de la phase d'enregistrement de l'utilisateur.

L'interface utilisateur-terminal comporte un clavier permettant à l'utilisateur de composer, sur requête du terminal, le numéro d'appel associé au terminal mobile.

35 le terminal comporte :

- des moyens de transmission terminal pour transmettre au serveur le numéro d'appel associé au terminal mobile,
- des moyens de communication terminal pour communiquer un mot de passe à l'utilisateur, notamment en affichant le mot de passe sur un écran du terminal ou en délivrant à l'utilisateur un ticket sur lequel est imprimé le mot de passe.

le mot de passe a été déterminé par le serveur en mettant en œuvre des moyens de traitement informatique.. le mot de passe a été transmis par le serveur au terminal, via le réseau de communication. Il résulte de la combinaison des traits techniques que le mot de passe attribué par le serveur ne peut être transmis qu'à l'utilisateur titulaire de l'objet portable authentifié. les moyens de traitement informatique serveur comportent des moyens d'enregistrement pour mémoriser et associer dans la base de données :

- les données d'identification,
- le numéro d'appel associé au terminal mobile,
- le mot de passe.

20 Phase de paiement

Pour permettre d'effectuer un paiement à distance auprès d'un accepteur, le système comprend des moyens de transmission accepteur permettant à l'utilisateur de transmettre à l'accepteur le numéro d'appel associé au terminal mobile.

25 le serveur de l'organisme comprend en outre :

- des moyens de réception serveur pour recevoir de l'accepteur le numéro d'appel associé au terminal mobile ainsi que des informations relatives au paiement, dont le montant du paiement,

30 - des moyens de transmission serveur pour adresser à l'utilisateur un message, notamment de type SMS, en utilisant le numéro d'appel associé au terminal mobile.

Le message comprend les informations relatives au paiement et une requête de saisie du mot de passe, se présentant 35 notamment sous la forme d'un champ de saisie dans le message.

Le terminal mobile comprend des moyens de transmission terminal mobile permettant, à l'utilisateur, de transmettre en retour le mot de passe au serveur de l'organisme, après que le mot de passe ait été saisi par l'utilisateur dans le champ de saisie.

Les moyens de traitement informatique serveur comportent :

- des moyens de vérification pour vérifier dans la base de données que le mot de passe transmis par l'utilisateur, correspond au numéro d'appel associé au terminal mobile transmis par l'accepteur,

- des moyens de recherche pour rechercher, dans la base de données, tout ou partie des données d'identification, notamment le numéro et la date d'expiration de l'objet portable, correspondant au numéro d'appel associé au terminal mobile et au mot de passe,

- des moyens de commande pour débiter ou pour faire débiter un compte bancaire associé à l'objet portable du montant du paiement et pour créditer ou pour faire créditer l'accepteur du montant.

- des moyens de transmission serveur pour confirmer à l'accepteur le paiement à distance de l'utilisateur.

De préférence, l'organisme vérifie la validité de l'objet portable avant de confirmer à l'accepteur le paiement à distance de l'utilisateur.

Il résulte de la combinaison des traits techniques que le paiement est acquitté à distance par l'utilisateur sans qu'il ait eu à communiquer à l'accepteur les données d'identification de l'objet portable, notamment le numéro et de la date d'expiration de la carte bancaire de l'utilisateur.

Grâce au procédé et au système selon l'invention, un commerçant accepteur à la possibilité de demander à un client utilisateur de s'inscrire au système de paiement en toute confiance selon l'invention, quel que soit l'émetteur de la carte. En effet, les clients utilisateurs peuvent utiliser des

DAB-GAB qui sont disponibles sur tout un territoire. Cette inscription ne constitue donc pas une contrainte très forte pour les clients utilisateurs. Ils peuvent l'accepter.

5 Dans ses conditions, le titulaire de la carte n'a plus de motif légitime de répudiation.

Par ailleurs, l'enregistrement est basé sur une authentification forte du client utilisateur et le paiement est fortement authentifié par le mot de passe connu du seul titulaire de la carte... Il est clair qu'un fraudeur aurait de 10 grande difficultés à effectuer des paiements avec la carte à l'insu du titulaire de la carte.

10 D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description de variantes de réalisation de l'invention données à titre d'exemple indicatif et non limitatif, et de la

15 - figure 1 qui représente un système permettant de valider qu'une requête auprès d'une entité émane d'un utilisateur habilité,
- figure 2 qui représente un système permettant à un 20 utilisateur habilité d'effectuer un paiement à distance auprès d'un accepteur.

On va maintenant décrire la figure 1 qui représente un système permettant de valider, en mettant en œuvre un objet portable 1 d'un utilisateur 2, qu'une requête 3 auprès d'une 25 entité 4 émane de cet utilisateur 2. L'objet portable 1 se présente notamment sous la forme d'une carte bancaire 5.

Dans le cas de la variante de réalisation décrite en 30 se référant à la figure 1, la requête 3 porte sur des informations confidentielles relatives à l'accès à un service ou à un lieu 6.

Dans le cas de la variante de réalisation qui sera décrite ci-après en se référant à la figure 2, la requête 3 porte sur une transaction.

35 On peut distinguer trois phases impliquant la mise en œuvre de moyens techniques spécifiques :

- une phase d'enregistrement au cours de laquelle l'utilisateur 2 s'enregistre auprès d'un organisme 7, notamment un organisme bancaire,

5 - une phase d'émission d'une requête 3,
- une phase d'autorisation de réponse à la requête 3.
Les éléments techniques mis en œuvre dans le cas de chacune des ces trois phases sont ci-après décrits.

Phase d'enregistrement de l'utilisateur 2 auprès d'un organisme 7.

10 Le système comprend, pour permettre l'enregistrement de l'utilisateur 2, un terminal 8, notamment un terminal de type distributeur automatique de billets (DAB-GAB) ou de type terminal de paiement électronique (TPE). Le terminal 8 comporte des moyens d'accouplement 26 permettant à l'utilisateur 2 de 15 accoupler l'objet portable 1 au terminal 8. Le système comprend en outre un serveur 9 associé à une base de données 10 gérée par l'organisme bancaire 7. Le serveur 9 comprend des moyens de connexion 27 qui permettent de connecter, de manière directe ou indirecte, le terminal 8 au serveur 9 via un réseau 20 de communication 28, notamment informatique. Le terminal 8 comprend une interface utilisateur-terminal 29 permettant à l'utilisateur 2 d'entrer dans le terminal 8, sur requête du terminal 8, des données d'authentification 11 de l'utilisateur, notamment un code confidentiel et/ou des données bio-métriques, 25 associées à l'objet portable 1. Le terminal 8 comprend en outre des moyens de vérification terminal 30 pour vérifier que les données d'authentification 11 de l'utilisateur 2 correspondent à l'objet portable 1.

30 Les moyens techniques ci-dessus décrits permettent donc d'authentifier l'objet portable 1 et de vérifier que l'utilisateur 2 qui s'enregistre est bien titulaire de l'objet portable 1.

35 L'interface utilisateur-terminal 29 comporte un clavier 12 permettant à l'utilisateur 2 de composer, sur requête du terminal 8, un identifiant personnel 13. Dans le cas de la

variante de réalisation représentée sur la figure 1, l'identifiant personnel 13 est le numéro d'appel associé au téléphone mobile 36 de l'utilisateur.

le terminal 8 comporte en outre :

5 - des moyens de transmission terminal 31 pour transmettre l'identifiant personnel 13 au serveur 9,
- des moyens de communication terminal 32 pour communiquer un mot de passe 15 à l'utilisateur, notamment en affichant le mot de passe 15 sur un écran 16 du terminal 8 ou en 10 délivrant à l'utilisateur 2 un ticket 17 sur lequel est imprimé le mot de passe 15.

15 le mot de passe 15 a été déterminé par le serveur 9 en mettant en œuvre des moyens de traitement informatique serveur 33. le mot de passe 15 a été transmis par le serveur 9 au terminal 8, via le réseau de communication 28.

20 Il résulte de la combinaison des moyens techniques ci-dessus décrits que le mot de passe 15 attribué par le serveur 9 ne peut être transmis qu'à l'utilisateur 2 titulaire de l'objet portable 1 préalablement authentifié.

25 Dans le cas où l'objet portable est une carte bancaire, on utilise un mécanisme d'authentification de la carte et de son titulaire qui existe en standard. On peut aller plus loin en effectuant une demande d'autorisation de paiement, ce qui permet de mettre en œuvre une mécanisme d'authentification supplémentaire impliquant alors la banque émettrice de la carte bancaire.

30 les moyens de traitement informatique serveur 33 comportent des moyens d'enregistrement 34 pour mémoriser et associer dans la base de données 10 :

- l'identifiant personnel 13,
- le mot de passe 15.

35 Dans le cas de la variante de réalisation représentée sur la figure 1 le terminal 8 comprend en outre des moyens de lecture terminal 43 permettant de lire dans l'objet portable 1 des données 20, notamment le numéro et la date d'expiration de

l'objet portable 1 ainsi que le nom et le prénom du titulaire de l'objet portable 1. Les moyens de transmission terminal 31 permettent de transmettre les données 20 ainsi lues au serveur 9. les moyens de lecture terminal 43 et les moyens de transmission terminal 31 sont mis en œuvre lors de la phase d'enregistrement de l'utilisateur. Les moyens d'enregistrement 34 du serveur 9 permettent de mémoriser dans la base de données 10 et d'associer avec l'identifiant personnel 13 et le mot de passe 15, les données 20, notamment le numéro et la date 10 d'expiration de l'objet portable 1.

Le système comprend en outre des moyens 35 d'établissement de requête 3 et de transmission de requête 3. Ces moyens 35 permettent à l'utilisateur 2 d'émettre une requête 3, concernant notamment des informations confidentielles d'accès 15 à un lieu 6, et de transmettre à l'entité 4 la requête 3 ainsi que l'identifiant personnel 13 de l'utilisateur 2. Dans le cas de la variante de réalisation représentée sur la figure 1, l'identifiant personnel 13 est le numéro d'appel 22 associé au téléphone mobile 36.

20 **Phase d'autorisation de réponse à la requête 3**

Les moyens techniques ci-après décrits sont mis en œuvre lors de la phase d'autorisation de réponse à la requête 3.

Le serveur 9 de l'organisme 7 comprend en outre :

- 25 - des moyens de réception serveur 37 pour recevoir de l'entité 4 l'identifiant personnel 13,
- des moyens de transmission serveur 38 pour adresser à l'utilisateur 2, via le téléphone mobile 36 de l'utilisateur, un message 18 de type SMS.

le message 18 comprend une requête de saisie du mot de passe 15 se présentant notamment sous la forme d'un champ de saisie 19 dans le message 18.

Le téléphone mobile 36 de l'utilisateur 2 comporte des moyens de transmission de mot de passe 50 permettant, à l'utilisateur, de transmettre en retour le mot de passe 15 au

serveur 9 de l'organisme 7. A cet effet, le mot de passe 15 est saisi par l'utilisateur 2 dans le champ de saisie 19.

Les moyens de traitement informatique serveur 33 comportent des moyens de vérification serveur 39 pour vérifier 5 dans la base de données 10 que le mot de passe 15, transmis par l'utilisateur, correspond à un mot de passe 15 associé à l'identifiant personnel 13 transmis par l'entité 4. Le serveur 9 produit, en cas de vérification aboutie, un message 10 d'autorisation 40 destiné à être transmis à l'entité 4, 15 l'autorisant à répondre à la requête 3 de l'utilisateur.

Dans le cas de la variante de réalisation représentée sur la figure 1, ainsi que cela a été déjà précisé, l'adresse de l'utilisateur 2 à laquelle l'organisme 7 peut transmettre la requête de saisie du mot de passe 15 est le numéro d'appel 22 15 associé au téléphone mobile de l'utilisateur 2. Ce numéro d'appel 22 de téléphone mobile constitue l'identifiant personnel 13. L'adresse constituant l'identifiant personnel 13 pourrait être d'une autre nature sans sortir du champ de l'invention. L'adresse pourrait par exemple être celle d'un téléphone fixe ou 20 l'adresse d'une messagerie électronique. Il résulte de la combinaison des moyens techniques décrits que, selon toute vraisemblance, le message 18 ne peut être reçu que par l'utilisateur.

Dans le cas de la variante de réalisation représentée 25 sur la figure 1, les moyens de traitement informatique serveur 33 et les moyens de transmission serveur 38 permettent de vérifier que l'utilisateur 2 peut être contacté à l'adresse définie par l'identifiant personnel 13.

On va maintenant décrire en se référant à la figure 2 30 une autre variante de réalisation du système selon l'invention. Dans le cas de la variante représentée sur la figure 2, le système permet à un utilisateur 2 d'effectuer un paiement à distance auprès d'un accepteur 23. A cet effet, l'utilisateur 2 dispose d'un objet portable 1 et d'un terminal mobile 25 ayant

une fonction de téléphonie. l'objet portable 1 se présente notamment sous la forme d'une carte bancaire 5.

On retrouve, dans le cas de la variante de réalisation représentée sur la figure 2 la plupart des mêmes organes que 5 ceux décrits en se référant à la figure 1. Ils portent les mêmes références numériques.

On peut distinguer, comme dans le cas de la variante de réalisation représentée sur la figure 1, deux phases impliquant la mise en œuvre de moyens techniques spécifiques :

10 - une phase d'enregistrement au cours de laquelle l'utilisateur 2 s'enregistre auprès d'un organisme 7, notamment un organisme bancaire,

- une phase de paiement.

Phase d'enregistrement de l'utilisateur 2 auprès d'un 15 organisme 7, notamment auprès d'un organisme bancaire

Le système comprend, pour permettre l'enregistrement de l'utilisateur, un terminal 8, notamment un terminal de type distributeur automatique de billets (DAB-GAB) ou de type terminal de paiement électronique (TPE). Le terminal 8 comporte 20 des moyens d'accouplement 26 permettant à l'utilisateur, d'accoupler l'objet portable 1 au terminal 8.

Le système comprend en outre un serveur 9 associé à une base de données 10 d'un organisme 7, notamment d'un organisme 7 bancaire.

25 le serveur 9 comprend des moyens de connexion 27 pour connecter, de manière directe ou indirecte, le terminal 8 au serveur 9 via un réseau de communication 28, notamment informatique.

le terminal 8 comprend en outre :

30 - une interface utilisateur-terminal 29 permettant à l'utilisateur 2 d'entrer dans le terminal 8, sur requête du terminal 8, des données d'authentification 11 de l'utilisateur, notamment un code confidentiel et/ou des données bio-métriques, associées à l'objet portable 1 ,

- des moyens de vérification terminal 30 pour vérifier que les données d'authentification 11 de l'utilisateur 2 correspondent à l'objet portable 1.

Il résulte de la combinaison des traits techniques que 5 la phase d'enregistrement permet d'authentifier l'objet portable 1 et de vérifier que l'utilisateur 2 est bien le titulaire de l'objet portable 1.

le terminal 8 comprend en outre :

- des moyens de lecture terminal 43 permettant de lire 10 dans l'objet portable 1 des données d'identification 20, notamment le numéro et la date d'expiration de l'objet portable 1 ainsi que le nom et le prénom du titulaire de l'objet portable 1,

15 - des moyens de transmission terminal 31 permettant de transmettre les données d'identification 20 au serveur 9.

Les moyens de lecture terminal 43 et les moyens de transmission terminal 31 sont mis en œuvre lors de la phase d'enregistrement de l'utilisateur.

L'interface utilisateur-terminal 29 comporte un 20 clavier 12 permettant à l'utilisateur 2 de composer, sur requête du terminal 8, le numéro d'appel associé au terminal mobile 25. dans le cas de la variante représentée sur la figure 2 le terminal mobile 25 est un téléphone mobile.

le terminal 8 comporte :

25 - des moyens de transmission terminal 31 pour transmettre au serveur 9 le numéro d'appel associé au terminal mobile 25,

- des moyens de communication terminal 32 pour 30 communiquer un mot de passe 15 à l'utilisateur, notamment en affichant le mot de passe 15 sur un écran 16 du terminal 8 ou en délivrant à l'utilisateur 2 un ticket 17 sur lequel est imprimé le mot de passe 15.

le mot de passe 15 a été déterminé par le serveur 9 en mettant en œuvre des moyens de traitement informatique. le mot 35 de passe 15 a été transmis par le serveur 9 au terminal 8, via

le réseau de communication 28. Il résulte de la combinaison des traits techniques que le mot de passe 15 attribué par le serveur 9 ne peut être transmis qu'à l'utilisateur 2 titulaire de l'objet portable 1 authentifié. les moyens de traitement informatique serveur 33 comportent des moyens d'enregistrement 34 pour mémoriser et associer dans la base de données 10 :

- les données d'identification 20,
- le numéro d'appel associé au terminal mobile 25,
- le mot de passe 15.

10 **Phase de paiement**

Pour permettre d'effectuer un paiement à distance auprès d'un accepteur 23, le système comprend des moyens de transmission accepteur 44 permettant à l'utilisateur 2 de transmettre à l'accepteur 23 le numéro d'appel 22 associé au terminal mobile 25.

Les moyens de transmission accepteur 44 peuvent être réalisés sous la forme d'un téléphone permettant à l'utilisateur 2 de transmettre vers un centre d'appel ou un serveur vocal le numéro d'appel 22 associé au terminal mobile 25. Ces données 20 peuvent être également transmises sous forme d'un message électronique au moyen d'un équipement informatique relié à un réseau de communication, notamment de type Internet. Les moyens de transmission accepteur 44 peuvent être des équipements différents du terminal mobile 25.

25 le serveur 9 de l'organisme 7 comprend en outre :
- des moyens de réception serveur 37 pour recevoir de l'accepteur 23 le numéro d'appel 22 associé au terminal mobile 25 ainsi que des informations relatives au paiement, dont le montant du paiement,

30 - des moyens de transmission serveur 38 pour adresser à l'utilisateur 2 un message 18, notamment de type SMS, en utilisant le numéro d'appel 22 associé au terminal mobile 25.

Le message 18 comprend les informations relatives au paiement et une requête de saisie du mot de passe 15, se

présentant notamment sous la forme d'un champ de saisie 19 dans le message 18.

Le terminal mobile 25 comprend des moyens de transmission terminal mobile 49 permettant, à l'utilisateur, de transmettre en retour le mot de passe 15 au serveur 9 de l'organisme 7, après que le mot de passe 15 ait été saisi par l'utilisateur 2 dans le champ de saisie 19.

Les moyens de traitement informatique serveur 33 comportent :

10 - des moyens de vérification serveur 39 pour vérifier dans la base de données 10 que le mot de passe 15, transmis par l'utilisateur, correspond au numéro d'appel associé au terminal mobile 25 transmis par l'accepteur 23,

15 - des moyens de recherche 47 pour rechercher, dans la base de données 10, tout ou partie des données d'identification 20, notamment le numéro et la date d'expiration de l'objet portable 1, correspondant au numéro d'appel associé au terminal mobile 25 et au mot de passe 15,

20 - des moyens de commande 48 pour débiter ou pour faire débiter un compte bancaire associé à l'objet portable 1 du montant du paiement et pour créditer ou pour faire créditer l'accepteur 23 du montant.

- des moyens de transmission serveur 38 pour confirmer à l'accepteur 23 le paiement à distance de l'utilisateur.

25 L'organisme 7 vérifie la validité de l'objet portable 1 avant de confirmer à l'accepteur 23 le paiement à distance de l'utilisateur.

Il résulte de la combinaison des traits techniques que le paiement est acquitté à distance par l'utilisateur 2 sans qu'il ait eu à communiquer à l'accepteur 23 les données d'identification 20 de l'objet portable 1, notamment le numéro et de la date d'expiration de la carte bancaire 5 de l'utilisateur.

30 Le procédé et le système selon l'invention permettent aux accepteurs (aux commerçants) qui le mettent en œuvre de se

passer du mode vente à distance classique car il est possible d'obtenir rapidement et simplement l'enregistrement préalable des utilisateurs au moyen de terminaux 8, notamment de distributeurs automatiques de billets DAB dispersés sur 5 l'ensemble du territoire. Les utilisateurs 2 peuvent ainsi accéder facilement au système et au procédé de paiement à distance selon l'invention.

La proportion dans laquelle le procédé et le système selon 10 l'invention réduira le taux d'impayé devrait être significative. En effet, les utilisateurs 2 sauront qu'on peut acheter et payer en toute confiance chez les accepteurs 23 (les commerçants) mettant en œuvre le procédé. Ils sauront non seulement que leur numéro de carte ne risque pas d'être compromis à cette occasion mais ils sauront également qu'aucun 15 fraudeur ne pourra acheter et payer selon le procédé de l'invention chez ces accepteurs 23 (commerçants) en utilisant un numéro de carte qui n'est pas le leur.

NOMENCLATURE

Groupe nominal	Réf. Num.
objet portable	1
utilisateur	2
requête	3
entité	4
carte bancaire	5
lieu	6
organisme	7
terminal	8
serveur	9
base de données	10
données d'authentification	11
clavier	12
identifiant personnel	13
mot de passe	15
écran	16
ticket	17
message	18
champ de saisie	19
données	20
données d'identification	20
Adresse/numéro d'appel	22
accepteur	23
terminal mobile	25
moyens d'accouplement	26
moyens de connexion	27
réseau de communication	28
interface utilisateur-terminal	29
moyens de vérification terminal	30
moyens de transmission terminal	31
moyens de communication terminal	32

BEST AVAILABLE COPY

moyens de traitement informatique	33
serveur	
moyens d'enregistrement	34
moyens d'établissement de requête (3) et de transmission de requête (3)	35
téléphone mobile	36
moyens de réception serveur	37
moyens de transmission serveur	38
moyens de vérification serveur	39
message d'autorisation	40
moyens de lecture terminal	43
moyens de transmission accepteur	44
moyens de recherche	47
moyens de commande	48
moyens de transmission terminal mobile	49
moyens de transmission de mot de passe	50

REVENDEDICATIONSProcédé

1. Procédé permettant de valider, en mettant en œuvre un objet portable (1) d'un utilisateur (2), qu'une requête (3) auprès d'une entité (4) émane dudit utilisateur (2) ; ledit objet portable (1) se présentant notamment sous la forme d'une carte bancaire (5) ; ladite requête (3) portant notamment sur une transaction ou des informations confidentielles relatives à l'accès à un service où à un lieu (6) ;

ledit procédé comprenant les étapes suivantes :

10 Phase d'enregistrement
 lors d'une phase d'enregistrement dudit utilisateur (2) auprès d'un organisme (7), notamment un organisme bancaire (7) :

15 - l'étape, pour ledit utilisateur (2), d'accoupler ledit objet portable (1) à un terminal (8), notamment de type distributeur automatique de billets (DAB-GAB) ou de type terminal (8) de paiement électronique (TPE) ; ledit terminal (8) étant connecté de manière directe ou indirecte à un serveur (9) associé à une base de données (10) dudit organisme (7) ;

20 ledit procédé comprenant en outre, lors de ladite phase d'enregistrement :

25 - l'étape, pour ledit utilisateur (2), sur requête dudit terminal (8), d'entrer dans ledit terminal (8) des données d'authentification (11) dudit utilisateur (2), notamment un code confidentiel et/ou des données bio-métriques, associées audit objet portable (1) ;

30 - l'étape, pour ledit terminal (8), de vérifier que lesdites données d'authentification (11) dudit utilisateur (2) correspondent audit objet portable (1) ;

 de sorte que la phase d'enregistrement permet d'authentifier l'objet portable (1) et de vérifier que l'utilisateur (2) est bien le titulaire de l'objet portable (1) ;
 ledit procédé comprenant en outre, lors de ladite phase d'enregistrement :

- l'étape, pour ledit utilisateur (2), sur requête dudit terminal (8), de composer, au moyen d'un clavier (12) dudit terminal (8), un identifiant personnel (13), notamment le numéro d'appel (22) d'un téléphone mobile (36) dudit utilisateur (2) ; ledit identifiant personnel (13) étant transmis par ledit terminal (8) audit serveur (9) ;
ledit procédé comprenant en outre :

- l'étape, pour ledit terminal (8), de transmettre un mot_de_passe (15), audit utilisateur (2), notamment en affichant ledit mot de passe (15) sur un écran (16) dudit terminal (8) ou en délivrant audit utilisateur (2) un ticket (17) sur lequel est imprimé ledit mot de passe (15) ; ledit mot de passe (15) ayant été déterminé par ledit serveur (9) et transmis audit terminal (8) ;

15 - de sorte que ledit mot de passe (15) attribué par le serveur (9) ne peut être transmis qu'audit utilisateur (2) titulaire de l'objet portable (1) authentifié ;
ledit procédé comprenant en outre, lors de ladite phase d'enregistrement :

20 - l'étape, pour ledit serveur (9), de mémoriser et d'associer, dans ladite base de données (10) dudit organisme (7) :

- ledit identifiant personnel (13),
- ledit mot de passe (15) ;

25 *Phase d'émission d'une requête (3)*
ledit procédé comprenant en outre, lors d'une phase d'émission d'une requête (3) concernant notamment des informations confidentielles :

- l'étape pour ledit utilisateur (2) de transmettre à ladite entité (4) :

- ladite requête (3),
- ledit identifiant personnel (13), notamment ledit numéro d'appel (22) associé audit téléphone mobile (36) ;

Phase d'autorisation de réponse à la requête (3)

ledit procédé comprenant en outre, lors d'une phase d'autorisation de réponse à la requête (3) :

- l'étape, pour ladite entité (4), de transmettre audit organisme (7) ledit identifiant personnel (13),
- 5 - l'étape, pour ledit organisme (7) d'adresser audit utilisateur (2) un message (18), notamment de type SMS ; ledit message (18) comprenant une requête de saisie dudit mot de passe (15), se présentant notamment sous la forme d'un champ de saisie (19) dans ledit message (18),
- 10 - l'étape, pour ledit utilisateur (2), de transmettre en retour ledit mot de passe (15) audit organisme (7), notamment en saisissant ledit mot de passe (15) dans ledit champ de saisie (19),
 - l'étape, pour ledit organisme (7), de vérifier dans 15 ladite base de données (10) que ledit mot de passe (15), transmis par ledit utilisateur (2), correspond à un mot de passe (15) associé audit identifiant personnel (13) transmis par ladite entité (4),
 - l'étape, pour ledit organisme (7), d'autoriser 20 ladite entité (4) à répondre à ladite requête (3) dudit utilisateur (2).

2. Procédé selon la revendication 1 ; ledit procédé étant tel qu'il comprend en outre, lors de la phase d'enregistrement, l'étape, pour ledit terminal (8), de lire dans 25 ledit objet portable (1) et de transmettre audit serveur (9) des données (20), notamment le numéro et la date d'expiration dudit objet portable (1) ainsi que le nom et le prénom du titulaire dudit objet portable (1).

3. Procédé selon la revendication 2; ledit procédé 30 étant tel qu'il comprend en outre l'étape pour le serveur (9) de mémoriser dans ladite base de données (10) dudit organisme (7) lesdites données (20), notamment ledit numéro et ladite date d'expiration dudit objet portable (1), et d'associer lesdites données (20) avec ledit identifiant personnel (13) et ledit mot de passe (15).

4. Procédé selon l'une quelconque des revendications 1 à 3; ledit procédé étant tel que ledit identifiant personnel (13) est une adresse dudit utilisateur (2) à laquelle ledit organisme (7) peut transmettre ladite requête de saisie dudit mot de passe (15); ladite adresse pouvant être notamment un numéro de téléphone mobile (36) ou de téléphone fixe ou une adresse de messagerie électronique.

5. Procédé selon la revendication 4; ledit procédé comprenant en outre l'étape, pour ledit organisme (7), de vérifier que ledit utilisateur (2) peut être contacté à l'adresse définie par ledit identifiant personnel (13), lors d'une requête relative audit identifiant personnel (13).

Cas du paiement de biens ou de services

6. Procédé destiné à permettre à un utilisateur (2), disposant d'un objet portable (1) et d'un terminal mobile (25) ayant une fonction de téléphonie, d'effectuer un paiement à distance auprès d'un accepteur (23); ledit objet portable (1) se présentant notamment sous la forme d'une carte bancaire (5); ledit procédé comprenant les étapes suivantes :

20. **phase d'enregistrement**
 lors d'une phase d'enregistrement dudit utilisateur (2) auprès d'un organisme (7), notamment un organisme bancaire (7) :

25. - l'étape, pour ledit utilisateur (2), d'accoupler ledit objet portable (1) à un terminal (8), notamment de type distributeur automatique de billets (DAB-GAB) ou de type terminal (8) de paiement électronique (TPE); ledit terminal (8) étant connecté de manière directe ou indirecte à un serveur (9) associé à une base de données (10) dudit organisme (7);

30. ledit procédé comprenant en outre, lors de ladite phase d'enregistrement :

 - l'étape, pour ledit utilisateur (2), sur requête dudit terminal (8), d'entrer dans ledit terminal (8) des données d'authentification (11) dudit utilisateur (2), notamment un code

confidentiel et/ou des données bio-métriques, associées audit objet portable (1),

5 - l'étape, pour ledit terminal (8), de vérifier que lesdites données d'authentification (11) dudit utilisateur (2), correspondent audit objet portable (1) ;

de sorte que la phase d'enregistrement permet d'authentifier l'objet portable (1) et de vérifier que l'utilisateur (2) est bien le titulaire de l'objet portable (1) ;

10 ledit procédé comprenant en outre :

- l'étape, pour ledit terminal (8), de lire dans ledit objet portable (1) et de transmettre audit serveur (9) des données d'identification (20), notamment le numéro et la date d'expiration dudit objet portable (1) ainsi que le nom et le 15 prénom du titulaire dudit objet portable (1),

20 - l'étape, pour ledit utilisateur (2), sur requête dudit terminal (8), de composer, au moyen d'un clavier (12) dudit terminal (8), le numéro d'appel (22) associé audit terminal mobile (25) ; ledit numéro d'appel (22) associé audit terminal mobile (25) étant transmis, par ledit terminal (8), audit serveur (9) ;

ledit procédé comprenant en outre :

25 - l'étape, pour ledit terminal (8), de transmettre un mot de passe (15) audit utilisateur (2), notamment en affichant ledit mot de passe (15) sur un écran (16) dudit terminal (8) ou en délivrant audit utilisateur (2) un ticket (17) sur lequel est imprimé ledit mot de passe (15) ; ledit mot de passe (15) ayant été déterminé par ledit serveur (9) et transmis audit terminal (8) ;

30 de sorte que ledit mot de passe (15) attribué par le serveur (9) ne peut être transmis qu'audit utilisateur (2) titulaire dudit objet portable (1) authentifié ;

ledit procédé comprenant en outre, lors de ladite phase d'enregistrement :

- l'étape, pour ledit serveur (9), de mémoriser et d'associer, dans ladite base de données (10) dudit organisme (7) :

- lesdites données d'identification (20),
- ledit numéro d'appel (22) associé audit terminal mobile (25),
- ledit mot de passe (15) ;

Phase de paiement

ledit procédé comprenant en outre lors d'une phase de 10 paiement :

- l'étape, pour ledit utilisateur (2), de transmettre audit accepteur (23) ledit numéro d'appel (22) associé audit terminal mobile (25) ;
- l'étape, pour ledit accepteur (23), de transmettre 15 audit organisme (7) ledit numéro d'appel (22) associé audit terminal mobile (25) ainsi que des informations relatives audit paiement, dont le montant dudit paiement,
- l'étape, pour ledit organisme (7) d'adresser audit utilisateur (2) un message (18), notamment de type SMS, en 20 utilisant ledit numéro d'appel (22) associé audit terminal mobile (25) ; ledit message (18) comprenant :
 - lesdites informations relatives audit paiement,
 - une requête de saisie dudit mot de passe (15), se présentant notamment sous la forme d'un champ de saisie (19) 25 dans ledit message (18),
- l'étape, pour ledit utilisateur (2), de transmettre en retour ledit mot de passe (15) audit organisme (7), notamment en saisisant ledit mot de passe (15) dans ledit champ de saisie (19),
- l'étape, pour ledit organisme (7), de vérifier dans 30 ladite base de données (10) que ledit mot de passe (15), transmis par ledit utilisateur (2), correspond audit numéro d'appel (22) associé audit terminal mobile (25) transmis par ledit accepteur (23),
- l'étape, pour ledit organisme (7) :

* de rechercher, dans ladite base de données (10), tout ou partie desdites données d'identification (20), notamment ledit numéro et ladite date d'expiration dudit objet portable (1), correspondant audit numéro d'appel (22) associé audit terminal mobile (25) et audit mot de passe (15),
5 * de faire débiter ou débiter un compte bancaire associé audit objet portable (1) du montant dudit paiement et de faire créditer ou créditer ledit accepteur (23) dudit montant ;
* de confirmer audit accepteur (23) ledit paiement à distance dudit utilisateur (2) ;
10 de sorte que le paiement est acquitté à distance par l'utilisateur (2) sans qu'il ait eu à communiquer à l'accepteur (23) les données d'identification (20) de l'objet portable (1), notamment le numéro et de la date d'expiration de la carte bancaire (5) de l'utilisateur (2).

Système

7. Système permettant de valider, en mettant en œuvre un objet portable (1) d'un utilisateur (2), qu'une requête (3) auprès d'une entité (4) émane dudit utilisateur (2) ; ledit 20 objet portable (1) se présentant notamment sous la forme d'une carte bancaire (5) ; ladite requête (3) portant notamment sur une transaction ou des informations confidentielles relatives à l'accès à un service ou à un lieu (6) ;

Phase d'enregistrement dudit utilisateur (2) auprès 25 d'un organisme (7), notamment un organisme bancaire (7) ledit système comprenant, pour permettre l'enregistrement dudit utilisateur (2) :
- un terminal (8), notamment un terminal (8) de type distributeur automatique de billets (DAB-GAB) ou de type 30 terminal (8) de paiement électronique (TPE), comportant des moyens d'accouplement (26) permettant audit utilisateur (2), d'accoupler ledit objet portable (1) audit terminal (8),
- un serveur (9) associé à une base de données (10) d'un organisme (7), notamment un organisme bancaire (7) ;

ledit serveur (9) comprenant des moyens de connexion (27) pour connecter, de manière directe ou indirecte, ledit terminal (8) audit serveur (9) via un réseau de communication (28), notamment informatique ;

5 ledit terminal (8) comprenant en outre :

- une interface utilisateur-terminal (29) permettant audit utilisateur (2) d'entrer dans ledit terminal (8), sur requête dudit terminal (8), des données d'authentification (11) dudit utilisateur (2), notamment un code confidentiel et/ou des 10 données bio-métriques, associées audit objet portable (1),
- des moyens de vérification terminal (30) pour vérifier que lesdites données d'authentification (11) dudit utilisateur (2) correspondent audit objet portable (1) ;

15 de sorte que la phase d'enregistrement permet d'authentifier l'objet portable (1) et de vérifier que l'utilisateur (2) est bien le titulaire de l'objet portable (1) ;
ledit terminal (8) étant tel que ladite interface utilisateur-terminal (29) comporte un clavier (12) permettant audit utilisateur (2) de composer, sur requête dudit terminal (8), un identifiant personnel (13), notamment le numéro d'appel (22) d'un téléphone mobile (36) dudit utilisateur (2) ;

20 ledit terminal (8) comportant :

- des moyens de transmission terminal (31) pour transmettre ledit identifiant personnel (13) audit serveur (9) ;
25 - des moyens de communication terminal (32) pour communiquer un mot de passe (15) audit utilisateur (2), notamment en affichant ledit mot de passe (15) sur un écran (16) dudit terminal (8) ou en délivrant audit utilisateur (2) un ticket (17) sur lequel est imprimé ledit mot de passe (15) ;
30 ledit mot de passe (15) ayant été déterminé par ledit serveur (9) en mettant en œuvre des moyens de traitement informatique serveur (33) ; ledit mot de passe (15) ayant été transmis par ledit serveur (9) audit terminal (8), via ledit réseau de communication (28) ;

de sorte que ledit mot de passe (15) attribué par le serveur (9) ne peut être transmis qu'à l'utilisateur (2) titulaire de l'objet portable (1) authentifié ;

lesdits moyens de traitement informatique serveur (33) 5 comportant des moyens d'enregistrement (34) pour mémoriser et associer dans ladite base de données (10) :

- ledit identifiant personnel (13),
- ledit mot de passe (15) ;

Phase d'émission d'une requête (3) par un utilisateur

10 (2)

ledit système comprenant en outre des moyens (35) d'établissement de requête (3) et de transmission de requête (3) permettant à l'utilisateur (2) d'émettre une requête (3), concernant notamment des informations confidentielles, et de 15 transmettre à ladite entité (4) ladite requête (3) ainsi que ledit identifiant personnel (13), notamment ledit numéro d'appel (22) associé audit téléphone mobile (36) ;

Phase d'autorisation de réponse à la requête (3)

10 autre :

- des moyens de réception serveur (37) pour recevoir de ladite entité (4) ledit identifiant personnel (13),
- des moyens de transmission serveur (38) pour adresser audit utilisateur (2) un message (18), notamment de 25 type SMS ; ledit message (18) comprenant une requête de saisie dudit mot de passe (15), se présentant notamment sous la forme d'un champ de saisie (19) dans ledit message (18) ;

ledit utilisateur disposant de moyens de transmission de mot de passe (50), notamment un téléphone mobile (36), 30 permettant, audit utilisateur (2), de transmettre en retour ledit mot de passe (15) audit serveur (9) dudit organisme (7), après que ledit mot de passe (15) ait été saisi par l'utilisateur (2) dans ledit champ de saisie (19) ;

lesdits moyens de traitement informatique serveur (33) 35 comportant des moyens de vérification serveur (39) pour vérifier

dans ladite base de données (10) que ledit mot de passe (15), transmis par ledit utilisateur (2), correspond à un mot de passe (15) associé audit identifiant personnel (13) transmis par ladite entité (4) ;

5 ledit serveur (9) produisant en cas de vérification aboutie un message d'autorisation (40), destiné à être transmis à ladite entité (4), l'autorisant à répondre à ladite requête (3) dudit utilisateur (2).

8. Système selon la revendication 7 ; ledit système 10 étant tel que ledit terminal (8) comprend :

- des moyens de lecture terminal (43) permettant de lire dans ledit objet portable (1) des données (20), notamment le numéro et la date d'expiration dudit objet portable (1) ainsi que le nom et le prénom du titulaire dudit objet portable (1),

15 - des moyens de transmission terminal (31) permettant de transmettre ledites données (20) audit serveur (9) ;

lesdits moyens de lecture terminal (43) et lesdits moyens de transmission terminal (31) étant mis en œuvre lors de la phase d'enregistrement dudit utilisateur (2).

20 9. Système selon la revendication 8 ; ledit système étant tel que lesdits moyens d'enregistrement (34) dudit serveur (9) permettent de mémoriser dans ladite base de données (10) et d'associer avec ledit identifiant personnel (13) et ledit mot de passe (15), lesdites données (20), notamment ledit numéro et 25 ladite date d'expiration dudit objet portable (1).

10. Système selon l'une quelconque des revendications 7 à 9 ; ledit système étant tel que ledit identifiant personnel (13) est une adresse dudit utilisateur (2) à laquelle ledit organisme (7) peut transmettre ladite requête de saisie dudit 30 mot de passe (15) ; ladite adresse pouvant être notamment un numéro de téléphone mobile (36) ou de téléphone fixe ou une adresse de messagerie électronique ;

de sorte que, selon toute vraisemblance, ledit message (18) ne peut être reçu que par l'utilisateur (2).

11. Système selon la revendication 10 ; ledit système étant tel que lesdits moyens de traitement informatique serveur (33) et lesdits moyens de transmission serveur (38) dudit serveur (9) permettent de vérifier que ledit utilisateur (2) peut être contacté à ladite adresse définie par ledit identifiant personnel (13).

Cas du paiement de biens ou de services

12. Système destiné à permettre à un utilisateur (2), disposant d'un objet portable (1) et d'un terminal mobile (25) ayant une fonction de téléphonie, d'effectuer un paiement à distance auprès d'un accepteur (23) ; ledit objet portable (1) se présentant notamment sous la forme d'une carte bancaire (5) ;

15 Phase d'enregistrement dudit utilisateur (2) auprès d'un organisme (7), notamment auprès d'un organisme bancaire (7)

ledit système comprenant, pour permettre l'enregistrement dudit utilisateur (2) :

- un terminal (8), notamment un terminal (8) de type distributeur automatique de billets (DAB-GAB) ou de type terminal (8) de paiement électronique (TPE), comportant des moyens d'accouplement (26) permettant audit utilisateur (2), d'accoupler ledit objet portable (1) audit terminal (8),

- un serveur (9) associé à une base de données (10) d'un organisme (7), notamment d'un organisme bancaire (7) ;

25 ledit serveur (9) comprenant des moyens de connexion (27) pour connecter, de manière directe ou indirecte, ledit terminal (8) audit serveur (9) via un réseau de communication (28), notamment informatique :

ledit terminal (8) comprenant en outre :

30 - une interface utilisateur-terminal (29) permettant d'entrer dans ledit terminal (8), sur requête dudit terminal (8), des données d'authentification (11) dudit utilisateur (2), notamment un code confidentiel et/ou des données bio-métriques, associées audit objet portable (1),

- des moyens de vérification terminal (30) pour vérifier que lesdites données d'authentification (11) dudit utilisateur (2), correspondent audit objet portable (1) ; de sorte que la phase d'enregistrement permet 5 d'authentifier l'objet portable (1) et de vérifier que l'utilisateur (2) est bien le titulaire de l'objet portable (1) ;

ledit terminal (8) comprenant en outre :

- des moyens de lecture terminal (43) permettant de lire dans ledit objet portable (1) des données d'identification 10 (20), notamment le numéro et la date d'expiration dudit objet portable (1) ainsi que le nom et le prénom du titulaire dudit objet portable (1),
- des moyens de transmission terminal (31) permettant 15 de transmettre lesdites données (20) audit serveur (9) ; lesdits moyens de lecture terminal (43) et lesdits moyens de transmission terminal (31) étant mis en œuvre lors de la phase d'enregistrement dudit utilisateur (2) ;

ledit terminal (8) étant tel que ladite interface 20 utilisateur-terminal (29) comporte un clavier (12) permettant audit utilisateur (2) de composer, sur requête dudit terminal (8), le numéro d'appel (22) associé audit terminal mobile (25) ;

ledit terminal (8) comportant :

- des moyens de transmission terminal (31) pour 25 transmettre audit serveur (9) ledit numéro d'appel (22) associé audit terminal mobile (25),
- des moyens de communication terminal (32) pour communiquer un mot de passe (15) audit utilisateur (2), notamment en affichant ledit mot de passe (15) sur un écran (16) 30 dudit terminal (8) ou en délivrant audit utilisateur (2) un ticket (17) sur lequel est imprimé ledit mot de passe (15) ;

ledit mot de passe (15) ayant été déterminé par ledit serveur (9) en mettant en œuvre des moyens de traitement informatique serveur (33) ; ledit mot de passe (15) ayant été 35

transmis par ledit serveur (9) audit terminal (8), via ledit réseau de communication (28) ;

de sorte que ledit mot de passe (15) attribué par le serveur (9) ne peut être transmis qu'audit utilisateur (2) titulaire dudit objet portable (1) authentifié ;

lesdits moyens de traitement informatique serveur (33) comportant des moyens d'enregistrement (34) pour mémoriser et associer dans ladite base de données (10) :

- 10 - lesdites données d'identification (20),
 - ledit numéro d'appel (22) associé audit terminal mobile (25),
 - ledit mot de passe (15) ;

Phase de paiement

ledit système comprenant des moyens de transmission accepteur (44) permettant audit utilisateur (2) de transmettre audit accepteur (23) ledit numéro d'appel (22) associé audit terminal mobile (25) ;
ledit serveur (9) dudit organisme (7) comprenant en outre :

- 20 - des moyens de réception serveur (37) pour recevoir dudit accepteur (23) ledit numéro d'appel (22) associé audit terminal mobile (25) ainsi que des informations relatives audit paiement, dont le montant dudit paiement,

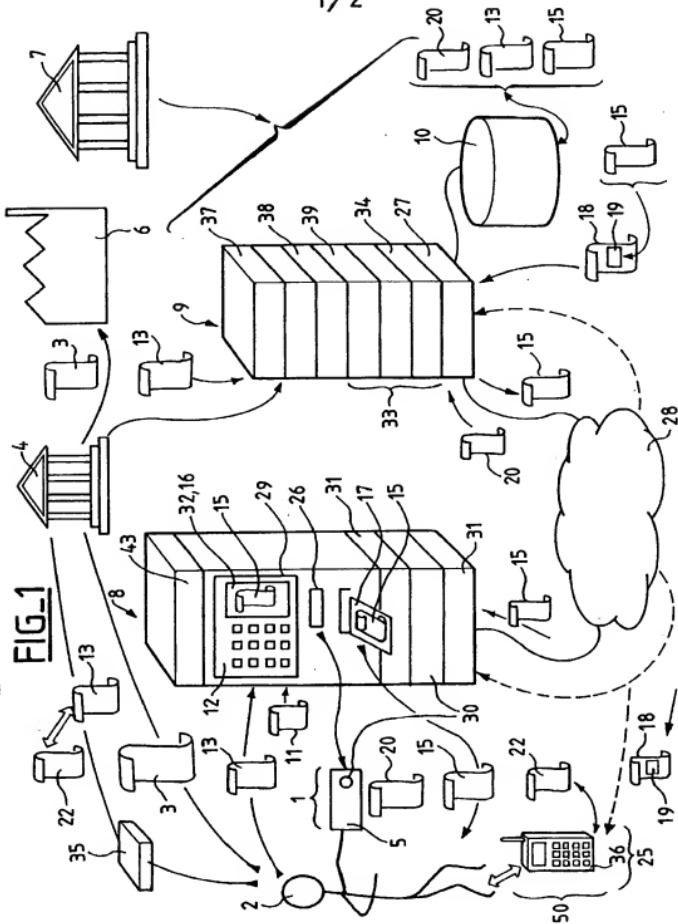
- des moyens de transmission serveur (38) pour adresser audit utilisateur (2) un message (18), notamment de type SMS, en utilisant ledit numéro d'appel (22) associé audit terminal mobile (25) ;

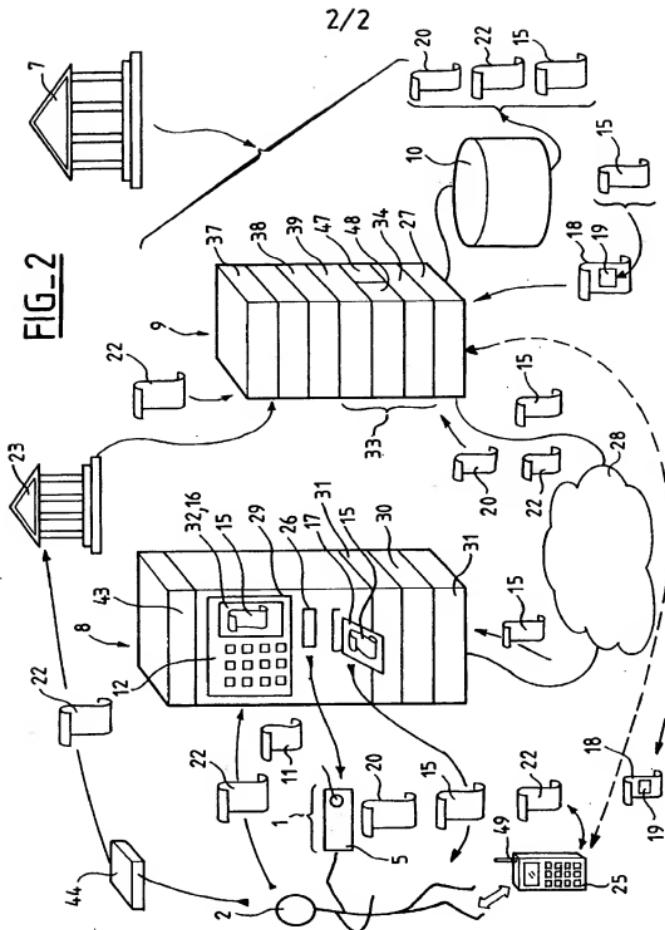
ledit message (18) comprenant lesdites informations relatives audit paiement et une requête de saisie dudit mot de passe (15), se présentant notamment sous la forme d'un champ de saisie (19) dans ledit message (18) ;

ledit terminal mobile (25) comprenant des moyens de transmission terminal mobile (49) permettant, audit utilisateur (2), de transmettre en retour ledit mot de passe (15) audit serveur (9) dudit organisme (7), après que ledit mot de passe

(15) ait été saisi par ledit utilisateur (2) dans ledit champ de saisie (19),
lesdits moyens de traitement informatique serveur (33) comportant :
5 - des moyens de vérification serveur (39) pour vérifier dans ladite base de données (10) que ledit mot de passe (15), transmis par ledit utilisateur (2), correspond audit numéro d'appel (22) associé audit terminal mobile (25) transmis par ledit accepteur (23),
10 - des moyens de recherche (47) pour rechercher, dans ladite base de données (10), tout ou partie desdites données d'identification (20), notamment ledit numéro et ladite date d'expiration dudit objet portable (1), correspondant audit numéro d'appel (22) associé audit terminal mobile (25) et audit mot de passe (15),
15 - des moyens de commande (48) pour débiter ou pour faire débiter un compte bancaire associé audit objet portable (1) du montant dudit paiement et pour créditer ou pour faire créditer ledit accepteur (23) dudit montant ;
20 lesdits moyens de transmission serveur desdits traitement informatique serveur (33) permettant de confirmer à l'accepteur le paiement à distance de l'utilisateur ;
de sorte que le paiement est acquitté à distance par l'utilisateur (2) sans qu'il ait eu à communiquer à l'accepteur (23) les données d'identification (20) de l'objet portable (1), notamment le numéro et de la date d'expiration de la carte bancaire (5) de l'utilisateur (2).

1/2





FEUILLE DE REMPLACEMENT (REGLE 26)

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
6 février 2003 (06.02.2003)

PCT

(10) Numéro de publication internationale
WO 03/010720 A3

(51) Classification internationale des brevets⁷ : G07F 7/10, 19/00

(72) Inventeurs; et
(75) Inventeurs/Déposants (pour US seulement) : BERGSTEN, Ulrik [FR/FR]; 17 rue Louis Maurice, F-94210 LA VARENNE (FR). ASSUERUS, Frédéric [FR/FR]; River Side, 74 rue Camille Claudel, F-78955 CARRIERES SOUS POISSY (FR).

(21) Numéro de la demande internationale : PCT/FR02/02657

(22) Date de dépôt international : 24 juillet 2002 (24.07.2002)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
01 09904 25 juillet 2001 (25.07.2001) FR
01 09903 25 juillet 2001 (25.07.2001) FR

(71) Déposant (pour tous les États désignés sauf US) : CREDIT LYONNAIS [FR/FR]; 18 rue de la République, F-69002 LYON (FR).

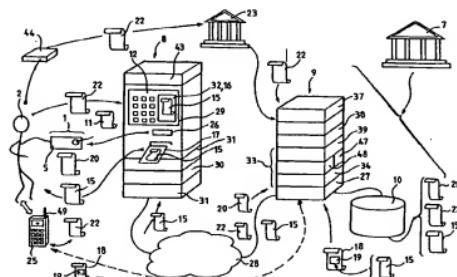
(74) Mandataire : GRYNWALD, Albert; Cabinet GRYNWALD, 127 rue du Faubourg Poissonnière, F-75009 PARIS (FR).

(81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

[Suite sur la page suivante]

(54) Title: METHOD AND SYSTEM USING A USER PORTABLE DEVICE FOR VALIDATING A REQUEST WITH AN ENTITY

(54) Titre : PROCÉDÉ ET SYSTÈME PERMETTANT DE VALIDER, EN METtant EN ŒUVRE UN OBJET PORTABLE D'UN UTILISATEUR, UNE REQUÊTE AUPRÈS D'UNE ENTITÉ



(57) Abstract: The invention concerns a method and a system enabling a user (2) to perform remote payment settlement for goods and/or services. The method comprises: a step whereby the user (2) transmits to an acceptor trader (23) supplying goods and/or services, a personal identifier, in particular consisting of a call number (22) of the mobile telephone (25) of the user (2); a step whereby the user (2) transmits a password (15) to a banking institution (7). When the user (2) is registered, the password (15) is transmitted, by the banking institution (7) to the user (2) entirely or partly via a terminal (8), in particular an ATM/ABM automatic cash dispensing machine. The payment for the goods and/or services is thus settled remotely by the user (2).

[Suite sur la page suivante]

WO 03/010720 A3



(84) États désignés (*régional*): brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :
— avec rapport de recherche internationale

(88) Date de publication du rapport de recherche internationale: 27 novembre 2003

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) **Abbrégé :** L'invention concerne un procédé et un système permettant à un utilisateur (2) d'acquitter à distance le paiement de biens et/ou de services. Le procédé comprend :- l'étape, pour l'utilisateur (2), de transmettre, à un commerçant accepteur (23) fournissant les biens et/ou services, un identifiant personnel, notamment constitué du numéro d'appel (22) du téléphone mobile (25) de l'utilisateur (2). - l'étape, pour l'utilisateur (2), de transmettre, directement ou indirectement, un mot de passe (15) à un organisme bancaire (7). Lors d'une phase d'enregistrement de l'utilisateur (2), le mot de passe (15) a été transmis, par l'organisme bancaire (7) à l'utilisateur (2), en tout ou partie via un terminal (8), notamment un distributeur automatique de billets de banque du type DAB/GAB. Le paiement des biens et/ou services est ainsi acquitté à distance par l'utilisateur (2).

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 02/02657

A. CLASSIFICATION OF SUBJECT MATTER
 IPC 7 G07F7/10 G07F19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHEDMinimum documentation searched (classification system followed by classification symbols)
 IPC 7 G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)
 EPO-Internal, WPI Data**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 01 39085 A (KLOOR HARRY THOMAS) 31 May 2001 (2001-05-31) page 6, line 29 - line 34 page 8, line 5 -page 11, line 11 claims 1,3,5,6,8,11,17 figures 2,3,5,9	1-12
A	WO 00 17794 A (CHEN ANN PIN ;VISA INT SERVICE ASS (US)) 30 March 2000 (2000-03-30) page 20, line 10 -page 21, line 18 page 22, line 7 - line 26 figures 1,2,5,6	1-12
A	US 5 986 565 A (ISAKA ISAO) 16 November 1999 (1999-11-16) column 4, line 3 -column 5, line 4 figure 2	1,4,5,7, 10,11
-/-		

 Further documents are listed in the continuation of box C. Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the International filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document relating to an oral disclosure, use, exhibition or other means
- *P* document published prior to the International filing date but later than the priority date claimed

T later document published after the International filing date or priority date and not in conflict with the application but which is considered to involve the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is considered in combination with one or more other documents, such combination being obvious to a person skilled in the art

Z document member of the same patent family

Date of the actual completion of the International search	Date of mailing of the International search report
30 January 2003	12/02/2003
Name and mailing address of the ISA	Authorized officer

European Patent Office, P.B. 5018 Patentkant 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
 Fax. (+31-70) 340-3016

Paraf, E

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 02/02657

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6 078 908 A (SCHMITZ KIM) 20 June 2000 (2000-06-20) column 6, line 58 -column 7, line 31 column 7, line 66 -column 8, line 65 figures 1,2 -----	1,4,5,7, 10,11
A	FR 2 801 995 A (DUVAL BRUNO) 8 June 2001 (2001-06-08) page 9, line 3 -page 11, line 5 figures -----	1,4,5,7, 10,11

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 02/02657

Patent document cited in search report		Publication date		Patent family member(s)		Publication date
WO 0139085	A	31-05-2001	AU WO	1928601 A 0139085 A1		04-06-2001 31-05-2001
WO 0017794	A	30-03-2000	AU CA EP WO	1091900 A 2345391 A1 1116151 A2 0017794 A2		10-04-2000 30-03-2000 18-07-2001 30-03-2000
US 5986565	A	16-11-1999	NONE			
US 6078908	A	20-06-2000	DE AT AU BR CN DE EP JP TW	19718103 A1 226346 T 6354598 A 9801177 A 1207533 A 59805939 D1 0875871 A2 10341224 A 425804 B		04-06-1998 15-11-2002 05-11-1998 20-03-2001 10-02-1999 21-11-2002 04-11-1998 22-12-1998 11-03-2001
FR 2801995	A	08-06-2001	FR AU WO	2801995 A1 2525001 A 0143092 A1		08-06-2001 18-06-2001 14-06-2001

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No

PCT/FR 02/02657

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
 CIB 7 G07F7/10 G07F19/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORÉE

Documentation minimale consultée (système de classification suivie des symboles de classement)

CIB 7 G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDÉRÉS COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 01 39085 A (KLOOR HARRY THOMAS) 31 mai 2001 (2001-05-31) page 6, ligne 29 - ligne 34 page 8, ligne 5 -page 11, ligne 11 revendications 1,3,5,6,8,11,17 figures 2,3,5,9	1-12
A	WO 00 17794 A (CHEN ANN PIN ;VISA INT SERVICE ASS (US)) 30 mars 2000 (2000-03-30) page 20, ligne 10 -page 21, ligne 18 page 22, ligne 7 - ligne 26 figures 1,2,5,6	1-12
A	US 5 986 565 A (ISAKA ISAO) 16 novembre 1999 (1999-11-16) colonne 4, ligne 3 -colonne 5, ligne 4 figure 2	1,4,5,7, 10,11

 Voir la suite du cadre C pour la fin de la liste des documents Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- *A document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- *E document antérieur, mais public à la date de dépôt international ou après cette date
- *L document pouvant jouer un rôle sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre publication pour une raison spécifique (telle qu'un indice)
- *O document se référant à une divulgarion orale, à un usage, à une exposition ou autres moyens
- *P document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

*T document ultérieur publié après la date de dépôt international ou la date de priorité et n'ayant pas contribué à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

*X document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

*Y document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

*Z document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

30 janvier 2003

Date d'expédition du présent rapport de recherche internationale

12/02/2003

Nom et adresse postale de l'administration chargée de la recherche internationale
 Office Européen des Brevets, P.B. 5016 Patentstaan 2
 NL - 2280 HV Rijswijk
 Tel (+31-70) 340-2040, Tx. 31 651 epo nl,
 Fax (+31-70) 340-3016

Fonctionnaire autorisé

Paraf, E

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No

PCT/FR 02/02657

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	US 6 078 908 A (SCHMITZ KIM) 20 juin 2000 (2000-06-20) colonne 6, ligne 58 -colonne 7, ligne 31 colonne 7, ligne 66 -colonne 8, ligne 65 figures 1,2 -----	1,4,5,7, 10,11
A	FR 2 801 995 A (DUVAL BRUNO) 8 juin 2001 (2001-06-08) page 9, ligne 3 -page 11, ligne 5 figures -----	1,4,5,7, 10,11

RAPPORT DE RECHERCHE INTERNATIONALE
Informations relatives aux membres de familles de brevets

Demande internationale No
PCT/FR 02/02657

Document brevet cité au rapport de recherche	Date de publication		Membre(s) de la famille de brevet(s)		Date de publication
WO 0139085	A	31-05-2001	AU WO	1928601 A 0139085 A1	04-06-2001 31-05-2001
WO 0017794	A	30-03-2000	AU CA EP WO	1091900 A 2345391 A1 1116151 A2 0017794 A2	10-04-2000 30-03-2000 18-07-2001 30-03-2000
US 5986565	A	16-11-1999	AUCUN		
US 6078908	A	20-06-2000	DE AT AU BR CN DE EP JP TW	19718103 A1 226346 T 6354598 A 9801177 A 1207533 A 59805939 D1 0875871 A2 10341224 A 425804 B	04-06-1998 15-11-2002 05-11-1998 20-03-2001 10-02-1999 21-11-2002 04-11-1998 22-12-1998 11-03-2001
FR 2801995	A	08-06-2001	FR AU WO	2801995 A1 2525001 A 0143092 A1	08-06-2001 18-06-2001 14-06-2001